WHAT IS CLAIMED IS:

1. A method for identifying conditions affecting a computer network, the network having a mechanism for sending packet bursts along a path in the network and receiving said packet bursts at an end of the path, the method comprising:

providing a plurality of example signatures, each of the example signatures corresponding to a network condition;

acquiring test data regarding propagation of test packets along the path;

creating a test signature from the test data;

comparing the test signature to the example signatures; and,

identifying at least one of the example signatures which matches the test signature according to a match criterion.

2. The method of claim 1 wherein comparing the test signature to the example signatures comprises computing a similarity measure between the test signature and each of the example signatures.

3. The method of claim 1 wherein

the test signature comprises a plurality of values,

each of the example signatures comprise a set of corresponding values and,

computing the similarity measure between the test signature and an example signature comprises computing a fit between each of the values of the test signature and the corresponding value of the example signature.

4. The method of claim 3 wherein computing a fit between a value of the test signature and a corresponding value of the example signature is performed by evaluating a function associated with the value.

5. The method of claim 3 wherein computing the fit between each of the values of the test signature and the corresponding value of the example signature comprises performing a computation substantially mathematically equivalent to:

$$G(x,m) = A\exp(-B(x-m)^2)$$

where x is a value in the test signature, m is the corresponding value of the example signature and A and B are coefficients.

6. The method of claim 3 wherein computing the fit between each of the values of the test signature and the corresponding value of the example signature comprises performing a computation substantially mathematically equivalent to:

$$G(x,C,m,\lambda) = \frac{C}{\lambda 2\pi}\exp\left(\frac{-(x-m)^2}{2\lambda^2}\right)$$

where x is a value in the test signature, m is the corresponding value of the example signature, and C and λ are coefficients.

7. The method of claim 6 wherein values for C and λ are associated with each corresponding value of the example signature and

performing the computation comprises using the values for $\boldsymbol{C}$ and λ associated with the corresponding value of the example signature with which the fit to a value of the test signature is being computed.

8. The method of claim 2 wherein computing a similarity measure comprises performing a chi-squared calculation.

9. The method of claim 2 comprising normalizing the similarity measures corresponding to the example signatures before identifying at least one of the example signatures which matches the test signature.

10. The method of claim 9 wherein normalizing the similarity measures is based at least in part upon the similarity measure that would be obtained in a lossless network.

11. The method of claim 10 wherein normalizing the similarity measures is based at least in part upon the similarity measure that would be obtained if the test signature and example signature were identical.

12. The method of claim 11 wherein normalizing the similarity measures comprises evaluating for each similarity measure:

$$F_{normalized} = \frac{(FIT - F_{no\ loss})}{(F_{match} - F_{no\ loss})}$$

where ***FIT*** is the similarity measure, $F_{normalized}$ is the normalized similarity measure, $F_{no\ loss}$ is the similarity measure that would be obtained if the test data reported no loss of packets and F_{match} is the similarity measure that would be obtained if the test signature and example signature were identical.

13. The method of claim 9 comprising adjusting one or more of the similarity measures based upon an individual set of rules associated with that similarity measure before identifying at least one of the example signatures which matches the test signature.

14. The method of claim 13 wherein the individual set of rules includes one or more rules based upon factors including one or more of: a number of ICMP network unreachable messages; a number of ICMP host unreachable messages; a number of ICMP destination unreachable messages; a number of ICMP port unreachable messages; a number of ICMP protocol unreachable messages; a number of ICMP fragmentation required messages; a number of ICMP TTL expired messages; a number of ICMP source quench messages; a number of ICMP redirect messages; a number of ICMP router advertisement messages; a number of ICMP parameter problem messages; a number of ICMP security

problem messages; a number of unsolicited packets; a number of out-of-sequence packets; a non-standard MTU detected; and a number of timed out packets.

15. The method of claim 1 wherein the test signature comprises, packet loss statistics for a plurality of positions within bursts of test packets of a first size.

16. The method of claim 15 wherein the test signature comprises, packet loss statistics for a plurality of positions within bursts of test packets of a second size.

17. The method of claim 16 wherein one of the first and second sizes is not more than three times a minimum packet size for the path.

18. The method of claim 17 wherein the other of the first and second sizes is within 10% of a maximum packet size for the path.

19. The method of claim 16 wherein one of the first and second sizes is within 10% of a maximum packet size for the path.

20. The method of claim 16 wherein the test signature comprises, packet loss statistics for a plurality of positions within bursts of test packets of a third size wherein the third size is intermediate the first and second sizes.

21. The method of claim 1 wherein the test signature comprises a mean packet loss for bursts of packets of each of a plurality of sizes.

22. The method of claim 21 comprising determining the mean packet loss, ***BrAvg*** substantially as follows:

$$BrAvg = \frac{\sum_{i=1}^{n} l_i}{n}$$

where n is a number of packets in each burst, l_i is the loss ratio for the i^{th} packet in the burst and i is an index which ranges over all of the packets in the burst.

23. The method of claim 1 wherein the test signature comprises a first moment of packet losses within bursts of packets of a given size.

24. The method of claim 1 wherein the test signature comprises a first moment of packet losses within bursts of packets for bursts of packets of each of a plurality of sizes.

25. The method of claim 24 comprising determining the first moment of packet losses, ***BrMom***, substantially as follows:

$$BrMom = \frac{\sum_{i=1}^{n} i \times l_i}{\sum_{i=1}^{n} l_i}$$

where l_i is the loss ratio for the i^{th} packet in the burst and i is an index which ranges over all of the packets in the burst.

26. The method of claim 1 wherein the test data includes data regarding the propagation of datagrams along the test path.

27. The method of claim 26 wherein the test signature comprises one or more packet loss statistics for the datagrams.

28. The method of claim 27 wherein the test data comprises information regarding the propagation of datagrams of a plurality of sizes along the test path and the test signature comprises packet loss statistics for datagrams of each of the plurality of sizes.

29. The method of claim 1 wherein the path is a closed path.

30. The method of claim 29 wherein the packets comprise ICMP ECHO packets.

31. The method of claim 6 wherein the test signature comprises a mean packet loss for bursts of packets of each of a plurality of sizes.

32. The method of claim 31 comprising determining the mean packet loss, ***BrAvg*** substantially as follows:

$$BrAvg = \frac{\sum_{i=1}^{n} l_i}{n}$$

where n is a number of packets in each burst, l_i is the loss ratio for the i^{th} packet in the burst and i is an index which ranges over all of the packets in the burst.

33. The method of claim 16 wherein the test signature comprises a first moment of packet losses within bursts of packets of the first size.

34. The method of claim 16 wherein the test signature comprises a first moment of packet losses within bursts of packets for bursts of packets of each of the first and second sizes.

35. The method of claim 34 comprising determining the first moment of packet losses, ***BrMom***, substantially as follows:

$$BrMom = \frac{\sum_{i=1}^{n} i \times l_i}{\sum_{i=1}^{n} l_i}$$

where l_i is the loss ratio for the i^{th} packet in the burst and i is an index which ranges over all of the packets in the burst.

36. The method of claim 16 wherein the plurality of example signatures comprise example signatures corresponding to two or more of: a small queues condition; a lossy condition; a half-full duplex conflict condition; a full-half duplex conflict condition; an inconsistent MTU condition; a long half-duplex link condition; and a media errors condition.

37. Apparatus for identifying conditions affecting a computer network, the network having a mechanism for sending packets in bursts along a path in the network and receiving the packet bursts at an end of the path, the apparatus comprising:

a data store holding a plurality of example signatures, each of the example signatures corresponding to a network condition;

an input for receiving test data regarding propagation of test packets along the path;

means for creating a test signature from the test data;

means for comparing the test signature to the example signatures; and,

means for identifying at least one of the example signatures which matches the test signature.

38. The apparatus of claim 37 wherein the means for identifying at least one of the example signatures which matches the test signature comprises an expert system and a rule base.

39. The apparatus of claim 38 wherein the rule base includes rules which accept as input additional information other than the test signature.

40. The apparatus of claim 39 wherein the additional information comprises one or more of: a number of ICMP network unreachable messages; a number of ICMP host unreachable messages; a number of ICMP destination unreachable messages; a number of ICMP port unreachable messages; a number of ICMP protocol unreachable messages; a number of ICMP fragmentation required messages; a number of ICMP TTL expired messages; a number of ICMP source quench messages; a number of ICMP redirect messages; a number of ICMP router advertisement messages; a number of ICMP parameter problem messages; a number of ICMP security problem messages; a number of unsolicited packets; a number of out-of-sequence packets; a non-standard MTU detected; and a number of timed out packets.

41. The apparatus of claim 37 wherein the example signatures comprise example signatures corresponding to two or more of: a small queues condition; a lossy condition; a half-full duplex conflict condition; a full-half duplex conflict condition; an inconsistent MTU condition; a long half-duplex link condition; and a media errors condition.

42. The apparatus of claim 40 wherein the means for comparing the test signature to the example signatures comprises means for calculating a similarity measure between the test signature and each of the example signatures.

43. The apparatus of claim 42 wherein the the test signature comprises a plurality of values, each of the example signatures comprise a set of corresponding values and, the means for calculating a similarity measure between the test signature and each of the example signatures comprises means for computing a fit between each of the values of the test signature and the corresponding value of the example signature.

44. The apparatus of claim 42 wherein the means for comparing the test signature to the example signatures comprises a neural network.

45. Apparatus for identifying conditions affecting a computer network, the network having a mechanism for sending packets in bursts along a path in the network and receiving the packet bursts at an end of the path, the apparatus comprising:

a data store holding a plurality of example signatures, each of the example signatures corresponding to a network condition;

an input for receiving test data regarding propagation of test packets along the path;

a test signature creation mechanism configured to create a test signature based upon the test data;

a comparison system configured to derive a similarity measure between a test signature and each of the plurality of example signatures; and,

a selection system configured to identify at least one of the example signatures which best matches the test signature.

46. The apparatus of claim 45 comprising a data processor wherein the test signature creation mechanism, comparison system, and selection system each comprise a set of software instructions in a program store accessible to the processor.

47. The apparatus of claim 45 wherein the example signatures comprise, packet loss statistics for a plurality of positions within bursts of test packets of a first size.

48. The apparatus of claim 47 wherein the example signatures comprise packet loss statistics for a plurality of positions within bursts of test packets of a second size.

49. The apparatus of claim 48 wherein the example signatures comprise packet loss statistics for a plurality of positions within bursts of test packets of a third size wherein the third size is intermediate the first and second sizes.

50. The apparatus of claim 49 wherein the example signatures comprise a mean packet loss for bursts of packets of each of a plurality of sizes.

51. The apparatus of claim 49 wherein the example signatures comprise a first moment of packet losses within bursts of packets of a size.

52. The apparatus of claim 49 wherein the example signatures comprise a first moment of packet losses within bursts of packets for bursts of packets of each of a plurality of sizes.

53. The apparatus of claim 49 comprising a test packet sequencer connected to dispatch a sequence of test packets along a network path.

54. The apparatus of claim 53 wherein the test packet sequencer is configured to generate and to dispatch onto the path multiple bursts of ICMP ECHO packets.

55. The apparatus of claim 45 comprising a set weighting coefficients, fitting coefficients, or both weighing and fitting coefficients associated with one or more of the example signatures.

56. A program product comprising a computer readable medium carrying a set of computer-readable signals comprising instructions

which, when executed by a computer processor, cause the data processor to execute a method for identifying conditions affecting a computer network, the network having a mechanism for sending packet bursts along a path in the network and receiving said packet bursts at an end of the path, the method comprising:

providing a plurality of example signatures, each of the example signatures corresponding to a network condition;

acquiring test data regarding propagation of test packets along the path;

creating a test signature from the test data;

comparing the test signature to the example signatures; and,

identifying at least one of the example signatures which matches the test signature according to a match criterion.